

Jakobsson 38-2

AF/3621  
H/O  
H/O  
5  
C. Miller

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): B.M. Jakobsson et al.  
Case: 38-2  
Serial No.: 09/727,904  
Filing Date: December 1, 2000  
Group: 3621  
Examiner: Bradley B. Bayat

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: V. Bencivenga Date: April 26, 2004

Title: Tagged Private Information Retrieval

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

RECEIVED  
APR 30 2004

GROUP 3600

Sir:

Submitted herewith are the following documents relating to the above-identified patent application:

- (1) Appeal Brief in triplicate (original and two copies); and
- (2) Copy of Notice of Appeal, filed on February 24, 2004, with copy of stamped return postcard indicating receipt of Notice by PTO on February 26, 2004.

There is an additional fee of \$330 due in conjunction with this submission under 37 CFR §1.17(c). Please charge **Ryan, Mason & Lewis, LLP Account No. 50-0762** the amount of \$330, to cover this fee. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Deposit Account No. 50-0762** as required to correct the error. A duplicate copy of this letter and two copies of the Appeal Brief are enclosed.

04/28/2004 EFLDRES 00000074 500762 09727904

01 FC:1402

330.00 DA

Date: April 26, 2004

Respectfully submitted,

Joseph B. Ryan  
Attorney for Applicant(s)  
Reg. No. 37,922  
Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560  
(516) 759-7517



Jakobsson 38-2

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**Patent Application**

Applicant(s): B.M. Jakobsson et al.  
Case: 38-2  
Serial No.: 09/727,904  
Filing Date: December 1, 2000  
Group: 3621  
Examiner: Bradley B. Bayat

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Signature: V. Beniciver Date: April 26, 2004

Title: Tagged Private Information Retrieval

APPEAL BRIEF

Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

**RECEIVED**  
APR 30 2004  
**GROUP 3600**

Sir:

Applicants hereby appeal the final rejection dated November 24, 2003 of claims 1-20 of the above-identified application.

REAL PARTY IN INTEREST

The present application is assigned to Lucent Technologies Inc., as evidenced by an assignment recorded March 30, 2001 in the U.S. Patent and Trademark Office at Reel 011661, Frame 0358. The assignee Lucent Technologies Inc. is the real party in interest.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences.

### STATUS OF CLAIMS

The present application was filed on December 1, 2000 with claims 1-20. Claims 1-20 are currently pending in the application. Claims 1 and 16-20 are the independent claims.

Each of claims 1-20 stands rejected under 35 U.S.C. §103(a). Claims 1-20 are appealed.

### STATUS OF AMENDMENTS

There have been no amendments filed subsequent to the final rejection.

### SUMMARY OF INVENTION

The present invention is directed to arrangements for controlling access to one or more information items purchasable from a merchant and accessible over a network. In one aspect of the invention, a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, and the signed ciphertext has at least a first ciphertext portion.

An illustrative embodiment is implemented in a system 100 as shown in FIG. 1 of the drawings. In the system 100, a merchant 102, having associated therewith respective private and public databases 110, 112 and a payment server 114, interacts with a user device 122 over a network 120. A user comprising or otherwise associated with user device 122 purchases an information item from the merchant 102 in the manner illustrated in the flow diagram of FIG. 3, as described in the corresponding text at page 7, line 20, to page 9, line 21.

Generally, the merchant receives from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant. The merchant decrypts the blinded version of the first ciphertext portion and returns to the user the resulting decrypted blinded version of the first ciphertext portion. The resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

Such an arrangement provides a number of significant advantages over conventional techniques. For example, it “ensures that no one other than the user is able to determine what

particular information item has been purchased” (Specification, page 3, lines 10-11). This advantage is more particularly described as follows, in the context of the illustrative embodiment, at page 8, lines 23-29, of the specification:

The above-described blinding is an important feature of the invention, since it allows the sale of the information item  $m_i$  in a private manner, i.e., without anyone other than the user, i.e., customer 106, learning what information was sold, and without the possibility of any electronic or paper “trail” being created. More particularly, the payment server 114 and the merchant 102 do not know and cannot determine what retrievable information item the user has purchased. The invention thus provides strong protection of user privacy for purchase of retrievable information items over the Internet or other type of network.

#### ISSUES PRESENTED FOR REVIEW

1. Whether claims 1-20 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent No. 5,754,656 (hereinafter “Nishioka”) in view of U.S. Patent No. 6,275,936 (hereinafter “Kyojima”).
2. Whether claims 5 and 6 are unpatentable under §103(a) over Nishioka and Kyojima in view of U.S. Patent No. 6,396,928 (hereinafter “Zheng”).

#### GROUPING OF CLAIMS

With regard to Issue 1, claims 1, 4-6, 8, 9 and 15-17 stand or fall together, claim 2 stands or falls alone, claim 3 stands or falls alone, claim 7 stands or falls alone, claim 10 stands or falls alone, claim 11 stands or falls alone, claim 12 stands or falls alone, claim 13 stands or falls alone, claim 14 stands or falls alone, and claims 18-20 stand or fall together.

With regard to Issue 2, claims 5 and 6 stand or fall together.

#### ARGUMENT

##### Issue 1

A proper *prima facie* case of obviousness requires that the cited references when combined must “teach or suggest all the claim limitations,” and that there be some suggestion or motivation,

either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference teachings. See Manual of Patent Examining Procedure (MPEP), Eighth Edition, August 2001, §706.02(j).

Applicants submit that the Examiner has failed to establish a proper *prima facie* case of obviousness in the present §103(a) rejection of independent claims 1 and 16-20, in that the Nishioka and Kyojima references, even if assumed to be combinable, fail to teach or suggest all the claim limitations, and in that no cogent motivation has been identified for modifying the reference teachings to reach the claimed invention. Further, even if it is assumed that a proper *prima facie* case has been established, there are particular teachings in one or more of the references which controvert the obviousness argument put forth by the Examiner.

Independent claim 1 is directed to a method for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, and the signed ciphertext has at least a first ciphertext portion. The method includes the following steps, denoted (a) and (b) herein for ease of discussion:

(a) receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

(b) decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

As indicated above, an important advantage of the claimed arrangement relative to conventional techniques is that it “ensures that no one other than the user is able to determine what particular information item has been purchased” (Specification, page 3, lines 10-11).

The Examiner in formulating the §103(a) rejection of claim 1 acknowledges that the Nishioka reference fails to teach or suggest the claimed use of a blinded version of a first ciphertext portion of a signed ciphertext, as set forth in steps (a) and (b) of claim 1, but argues that these missing teachings are provided by Kyojima. Applicants respectfully disagree.

The Examiner specifically relies on the teachings of Kyojima in column 4, lines 57-67, as well as in columns 5-14 and the accompanying figures. Column 4, lines 57-67 of Kyojima provides as follows:

The present invention has been made in view of the above circumstances and has an aspect to provide a blind decryption that can securely transmit a specific piece of information to a decryption device while keeping the blindness of data delegated to be decrypted.

There is no teaching or suggestion in the above portion of Kyojima, or in the other portions of Kyojima relied upon by the Examiner, regarding the claimed use of a blinded version of a first ciphertext portion of a signed ciphertext of a given information item purchasable from a merchant. Instead, Kyojima simply discloses a particular blind decryption technique. Applicants have been unable to find any mention whatsoever in Kyojima regarding a signed ciphertext, much less a blinded version of a first ciphertext portion of a signed ciphertext as claimed.

It is therefore apparent that Nishioka and Kyojima, even if assumed to be combinable, fail to teach or suggest limitations (a) and (b) of claim 1 which relate to processing of a blinded version of a first ciphertext portion of a signed ciphertext of a given information item purchasable from a merchant. In fact, the collective teachings of these references fail to even mention a signed ciphertext.

Claim 1 thus includes one or more limitations which are not taught or suggested by the proposed combination of Nishioka and Kyojima. The combined teachings of these references therefore fail to “teach or suggest all the claim limitations” as would be required by a proper §103(a) rejection.

Also, as indicated previously, the Examiner has failed to identify a cogent motivation for modifying the reference teachings to reach the claimed invention. Neither Nishioka nor Kyojima

makes any mention regarding processing of a blinded version of a first ciphertext portion of a signed ciphertext of a given information item purchasable from a merchant. However, the Examiner states that it would be obvious to modify the teachings of these references to include the limitations in question because “one of ordinary skill in the art would recognize the benefit of utilizing a blind ciphertext decryption method to accomplish access control and authentication to digital data without disclosing unnecessary purchase information” (Final Office Action, page 5, first paragraph).

The Federal Circuit has stated that when patentability turns on the question of obviousness, the obviousness determination “must be based on objective evidence of record” and that “this precedent has been reinforced in myriad decisions, and cannot be dispensed with.” In re Sang-Su Lee, 277 F.3d 1338, 1343 (Fed. Cir. 2002). Moreover, the Federal Circuit has stated that “conclusory statements” by an examiner fail to adequately address the factual question of motivation, which is material to patentability and cannot be resolved “on subjective belief and unknown authority.” Id. at 1343-1344. There has been no showing in the present § 103(a) rejection of objective evidence of record that would motivate one skilled in the art to modify the proposed combination of Nishioka and Kyojima to produce the particular limitations in question. The above-quoted statement of obviousness given by the Examiner in the final Office Action is precisely the type of subjective, conclusory statement that the Federal Circuit has indicated provides insufficient support for an obviousness rejection.

Further, even if it is assumed that a proper *prima facie* case has been established, there are particular teachings in one or more of the references which controvert the obviousness argument put forth by the Examiner. As characterized by the Examiner, Nishioka discloses an arrangement in which “selective information relating to a purchase request by a user is only known to a merchant and certain authentication information is obtained by a payment center” (Final Office Action, page 4, last paragraph, with emphasis supplied). Assuming for purposes of argument that this characterization of Nishioka is correct, it represents a specific teaching away from the present invention as set forth in claim 1. As noted above, claim 1 specifies that the decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user. Since Nishioka, as characterized by the Examiner, teaches that an

information item purchased by a user can be identified by the merchant, it teaches away from the claimed invention, and teaches away from the proposed combination with Kyojima. Such a teaching away is believed to constitute strong evidence of non-obviousness.

Applicants therefore respectfully submit that independent claim 1 is allowable over Nishioka and Kyojima.

Independent claims 16 and 17 each include limitations corresponding to steps (a) and (b) above, and are therefore believed allowable for the reasons identified above with regard to independent claim 1.

Independent claims 18-20 recite limitations relating to a user purchase request which includes information generated using at least a portion of an encrypted version of a given information item purchasable from a merchant. Further, access to the given information item is provided in a manner such that the merchant is unable to identify the given information item purchased by the user. Such limitations are not taught or suggested by the combined teachings of Nishioka and Kyojima, for reasons similar to those described above with reference to claim 1. More specifically, these claims specify, among other limitations, that access to the given information item is provided in a manner such that the merchant is unable to identify the given information item purchased by the user. As indicated previously, the Examiner characterizes Nishioka as teaching that an information item purchased by a user can be identified by the merchant. Nishioka thus explicitly teaches away from the claimed invention and the proposed combination with Kyojima.

Claims 18-20 are therefore believed to be allowable over the proposed combination of Nishioka and Kyojima.

Dependent claims 2-15 are believed allowable for at least the reasons identified above with regard to independent claim 1, and these dependent claims are also believed to specify additional separately-patentable subject matter, as indicated below.

With regard to claim 2, this claim specifies that the signed ciphertext for the given information item comprises the first ciphertext portion, a second ciphertext portion, an unencrypted description of the information item, and a tag, with at least a portion of the tag comprising a signature. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 2, and Applicants have been unable to



find the claim 2 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 3, this claim specifies that the signature utilizes at least a part of the first ciphertext portion as a public key. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 3, and Applicants have been unable to find the claim 3 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 7, this claim specifies that the signed ciphertext further includes a second ciphertext portion corresponding to an encrypted version of the given information item. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 7, and Applicants have been unable to find the claim 7 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 10, this claim specifies that the decrypted blinded version of the first ciphertext portion returned to the user further comprises a proof of correct decryption that allows the user to check that the decrypted blinded version for correctness. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 10, and Applicants have been unable to find the claim 10 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 11, this claim specifies that the decrypted blinded version of the first ciphertext portion returned to the user comprises a blinded key that when unblinded by the user is used to decrypt a second ciphertext portion of the signed ciphertext so as to obtain the purchased information item. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 11, and Applicants have been unable to find the claim 11 limitations in the individual or collective disclosures of these references.

Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 12, this claim specifies that the decrypting step is implemented in at least part of a set of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding decryption result for each of the rounds. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 12, and Applicants have been unable to find the claim 12 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 13, this claim specifies that the decrypting step is implemented in  $j$  rounds, and wherein for each of the first  $j-1$  of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result that is subsequently reblinded by the user and provided as the blinded ciphertext for the next round, and wherein a plaintext generated after the  $j$ th round provides the information that is utilized by the user in conjunction with accessing the given information item. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 13, and Applicants have been unable to find the claim 13 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

With regard to claim 14, this claim specifies that the decrypting step is implemented in part of a set of  $j$  rounds, and wherein for each of the first  $j-1$  of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result, and wherein a plaintext generated after one of the first  $j-1$  rounds provides the information that is utilized by the user in conjunction with accessing the given information item. The Examiner fails to identify with specificity the particular portions of Nishioka or Kyojima which are alleged to meet the limitations of claim 14, and Applicants have been unable to find the claim 14 limitations in the individual or collective disclosures of these references. Applicants submit that the proposed combination of Nishioka and Kyojima fails to meet the limitations in question.

Issue 2

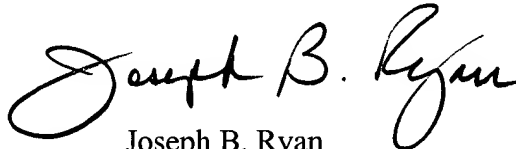
Applicants respectfully submit that the Zheng reference fails to supplement the above-described fundamental deficiency of the proposed combination of Nishioka and Kyojima as applied to independent claim 1.

Dependent claims 5 and 6 are therefore believed allowable at least by virtue of their dependence from independent claim 1.

Applicants further note that the Examiner has failed to demonstrate the requisite motivation for combining the Nishioka, Kyojima and Zheng references or modifying their teachings to reach the limitations in question.

In view of the above, Applicants believe that claims 1-20 are in condition for allowance, and respectfully request the withdrawal of the §103(a) rejections.

Respectfully submitted,

A handwritten signature in black ink, reading "Joseph B. Ryan". The signature is fluid and cursive, with the first name "Joseph" and last name "Ryan" clearly legible.

Date: April 26, 2004

Joseph B. Ryan  
Attorney for Applicant(s)  
Reg. No. 37,922  
Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560  
(516) 759-7517

## APPENDIX

1. A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext of the given information item, the signed ciphertext having at least a first ciphertext portion, the method comprising the steps of:

receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

decrypting the blinded version of the first ciphertext portion and returning to the user the resulting decrypted blinded version of the first ciphertext portion, wherein the resulting decrypted blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

2. The method of claim 1 wherein the signed ciphertext for the given information item comprises the first ciphertext portion, a second ciphertext portion, an unencrypted description of the information item, and a tag, with at least a portion of the tag comprising a signature.

3. The method of claim 2 wherein the signature utilizes at least a part of the first ciphertext portion as a public key.

4. The method of claim 1 wherein the first ciphertext portion comprises a symmetric key encrypted using a public key associated with the merchant.

5. The method of claim 1 wherein the first ciphertext portion is encrypted using an ElGamal encryption technique.

6. The method of claim 1 wherein the signed ciphertext is signed using a Schnorr signature.

7. The method of claim 1 wherein the signed ciphertext further includes a second ciphertext portion corresponding to an encrypted version of the given information item.

8. The method of claim 1 wherein the user verifies a signature of the signed ciphertext before requesting purchase of the given information item.

9. The method of claim 1 wherein the decrypting step is implemented in a payment server associated with the merchant.

10. The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user further comprises a proof of correct decryption that allows the user to check that the decrypted blinded version for correctness.

11. The method of claim 1 wherein the decrypted blinded version of the first ciphertext portion returned to the user comprises a blinded key that when unblinded by the user is used to decrypt a second ciphertext portion of the signed ciphertext so as to obtain the purchased information item.

12. The method of claim 1 wherein the decrypting step is implemented in at least part of a set of multiple rounds, with the user providing a blinded ciphertext and receiving a corresponding decryption result for each of the rounds.

13. The method of claim 12 wherein the decrypting step is implemented in  $j$  rounds, and wherein for each of the first  $j-1$  of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result that is subsequently reblinded by the user and provided as the blinded ciphertext for the next round, and wherein a plaintext generated after the  $j$ th round provides the information that is utilized by the user in conjunction with accessing the given information item.

14. The method of claim 12 wherein the decrypting step is implemented in part of a set of  $j$  rounds, and wherein for each of the first  $j-1$  of the rounds the user provides a blinded ciphertext and receives in response a corresponding decryption result, and wherein a plaintext generated after one of the first  $j-1$  rounds provides the information that is utilized by the user in conjunction with accessing the given information item.

15. The method of claim 1 wherein the merchant establishes different public keys for use with different ones of a plurality of information items purchasable from the merchant.

16. A processor-based system for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a signed ciphertext version of the given information item, the signed ciphertext version having at least a first ciphertext portion, and wherein the system is operative: (i) to receive from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and (ii) to decrypt the blinded version of the first ciphertext portion and return to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

17. A machine-readable medium containing one or more software programs for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein a user interested in a given information item is permitted to access a corresponding signed ciphertext having at least a first ciphertext portion, and wherein the one or more programs when executed implement the steps of:

receiving from the user a blinded version of the first ciphertext portion of the signed ciphertext in conjunction with a request from the user for purchase of the given information item from the merchant; and

decrypting the blinded version of the first ciphertext portion and returning to the user the resulting blinded version of the first ciphertext portion, wherein the resulting blinded version provides information that is utilized by the user in conjunction with accessing the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

18. A method for controlling access to one or more information items purchasable from a merchant and accessible over a network, the method comprising the steps of:

receiving from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and

returning to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

19. A processor-based system for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein the system is operative: (i) to



receive from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and (ii) to return to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.

20. A machine-readable medium containing one or more software programs for controlling access to one or more information items purchasable from a merchant and accessible over a network, wherein the one or more programs when executed implement the steps of:

receiving from the user a request for purchase of a given information item from the merchant, the request including information generated using at least a portion of an encrypted version of the given information item made accessible to the user without purchase of the given information item; and

returning to the user, in response to the request for purchase of the information item from the merchant, information that is utilized by the user to access the given information item in a manner such that the merchant is unable to identify the given information item purchased by the user.